Cryptshare
Making e-mail better

Kommentar

Angriffe auf Krankenhäuser über E-Mails: Das Problem ist Teil der Lösung

Eine Einschätzung von Matthias Kess, CTO der auf Kommunikationslösungen spezialisierten befine Solutions AG

Freiburg im Breisgau, 21. November 2018. Für knapp eineinhalb Wochen muss das Klinikum Fürstenfeldbruck vollständig ohne seine 450 Computer auskommen und ist auch nicht per E-Mail, sondern nur noch telefonisch erreichbar. Ursache ist wohl ein E-Mail-Trojaner, der über einen Anhang ins System eingedrungen ist. Inzwischen ermittelt die Zentralstelle Cybercrime Bayern, und das Klinikum hat alle Bankkonten sperren lassen. Wie in anderen bekannt gewordenen Fällen auch spielen E-Mails eine zentrale Rolle, sie sind nach wie vor das Haupteinfallstor für Schad-Software aller Art. Das ist Teil des Problems und kann Teil der Lösung sein – wenn Einrichtungen, Unternehmen und Behörden die Art ihrer Kommunikation ändern. Der Vorfall zeigt, dass die Sensibilisierung von Mitarbeitern für das Thema Cyber-Sicherheit unabdingbar ist, aber nicht isoliert betrachtet werden sollte.

Berichten zufolge fiel der erste Rechner des Krankenhauses aus, vermutlich nachdem ein E-Mail-Anhang mit einer darin versteckten Schadsoftware geöffnet wurde, danach hätten immer mehr Abteilungen Probleme gemeldet. Zwar ist die Versorgung der Patienten nach Angaben der Klinikleitung gewährleistet, allerdings hatte sich das einzige Krankenhaus in dem westlich von München gelegenen Landkreis von der Rettungsleitstelle abgemeldet, damit Ambulanzen nur noch lebensgefährlich verletzte Menschen dorthin brachten.

Horrorszenario: Komplettausfall einer Klinik-IT

Es ist zu vermuten, dass dahinter eine Infektion mit der Schad-Software Emotet steckt: Die auf Passwort-Diebstahl und Onlinebanking-Betrug spezialisierte Malware wird derzeit verstärkt in Rechnungen per E-Mail verbreitet. Egal ob gefälschte Rechnungen oder Bewerbungen – die Kriminellen versuchen immer, den Empfänger einer E-Mail dazu zu bringen, einen Dateianhang zu öffnen und auszuführen oder Links zu infizierten Webseiten anzuklicken.

Überhaupt spielt E-Mail hier eine zentrale Rolle: Sie hat sich speziell im Unternehmensumfeld seit vielen Jahren als Hauptkommunikationsmittel etabliert, ist einfach zu bedienen und universell verfügbar – und andererseits seit langem ein bevorzugtes Angriffsziel von Kriminellen, Hackern und Wirtschaftsspionen. Wie auch das aktuelle Beispiel zeigt, lauern die Gefahren in der Art, wie Mitarbeiter kommunizieren. Daher kommt es für IT-Verantwortliche darauf an, die Angriffsfläche zu verringern.

KRITIS: Ein kritischer Blick auf Kommunikationsprozesse ist nötig

Bisheriger „Höhepunkt“ ähnlicher Fälle war die „WannaCry“-Attacke im Mai 2017, bei der mehr als 300.000 Rechner in rund 150 Ländern infiziert worden waren. Getroffen hatte es Unternehmen in der Logistik, der Telekommunikation und dem Gesundheitswesen: In Großbritannien kam es beispielsweise zu erheblichen Störungen in der medizinischen Versorgung, während hierzulande Anzeigetafeln und Fahrkartenautomaten auf Bahnhöfen ausfielen. Ein Jahr vorher machte das Lukas-Krankenhaus im nordrhein-westfälischen Neuss Schlagzeilen, als ein Erpressungstrojaner alle IT-Systeme lahmlegte. Drastischer hätte uns die Verwundbarkeit der digitalen Infrastruktur wohl kaum vor Augen geführt werden können.

Wie eine Studie der Unternehmensberatung Roland Berger ergab, wurden knapp zwei Drittel der deutschen Krankenhäuser (64 Prozent) schon einmal Opfer eines Hacker-Angriffs. Es ist auffällig, dass sehr oft Systeme in so genannten „kritischen Infrastrukturen (KRITIS)“ infiziert wurden. Dazu zählen die großen Krankenhäuser, die in schwerwiegenden Fällen der Meldepflicht unterliegen.

Doch gerade hier tun sich die Betroffenen schwer, die immer wieder erhobenen Forderungen nach dem sofortigen Aktualisieren von Software umzusetzen. Vielmehr ist ein Perspektivenwechsel nötig – weg von der IT und hin zu den in vielen Unternehmen und Behörden vorherrschenden Kommunikationsprozessen.

Wie Einrichtungen, Behörden und Unternehmen die Angriffsfläche verringern können

Der aktuelle Vorfall zeigt erneut, dass die Sensibilisierung von Mitarbeitern für das Thema Cyber-Sicherheit in Form von regelmäßigen Schulungen unabdingbar ist, aber nicht isoliert betrachtet werden sollte.

Neben Informationen, die Angreifer aus den sozialen Medien ziehen, sind auch jene aus unverschlüsselten E-Mails ein Risiko. Und selbst bei verschlüsselten E-Mails (S/MIME und PGP) ist noch im Klartext ersichtlich, wer mit wem über welches Thema kommuniziert – über die Betreffzeile. Dies kann ausreichen, um einem der beiden Kommunikationsteilnehmer weitere Informationen zu entlocken, was für die Vorbereitung eines Social-Engineering-Angriffs genügen kann.

Hier bieten spezielle Software-Lösungen Schutz, mit deren Hilfe IT-Verantwortliche die Angriffsfläche von E-Mails verringern und so Kriminellen die Arbeit erheblich erschweren können. Eine spezielle Authentifizierung sowie das verschlüsselte Übertragen der Inhalte machen dann das Mitlesen von E-Mail-Korrespondenz unmöglich. Wenn auch die Betreffzeile verschlüsselt ist, können Angreifer nicht erkennen, wer mit wem worüber spricht und daraus Rückschlüsse ziehen – schon diese Informationen können ausreichen, um einen Social-Engineering-Angriff zu starten und mit dem gewonnenen Wissen einem der beiden Kommunikationsteilnehmer weitere Informationen zu entlocken. Zusätzlich wird es so äußerst schwer, Schad-Software einzuschleusen – eine Man-in-the-Middle-Attacke auf dem Weg einer Nachricht von A nach B, bei der die Zahlungsinformationen des eigentlichen Empfängers durch die der Kriminellen ersetzt werden, ist nahezu unmöglich.

Über Matthias Kess
Matthias Kess ist CTO der befine Solutions AG mit Sitz in Freiburg im Breisgau, die Kommunikationslösungen für Unternehmen entwickelt und vertreibt.

Über Cryptshare und befine Solutions
Die inhabergeführte befine Solutions AG entwickelt und vertreibt Softwarelösungen für Unternehmen, die damit ihre Prozesse unterstützen, optimieren und überwachen können. Hauptsitz und Entwicklungsstandort des im Jahr 2000 gegründeten Unternehmens mit über 50 Mitarbeitern ist Freiburg im Breisgau. Vertriebsstandorte gibt es in Großbritannien sowie den Niederlanden, eine Tochtergesellschaft in den USA.
Im Mittelpunkt steht Cryptshare, eine Kommunikationslösung für den sicheren Austausch von Informationen. Mit ihr lassen sich E-Mails und Dateien jeder Größe und Art ad-hoc austauschen – einfach und sicher, nachvollziehbar und kostengünstig. Sie ist in mehr als 1.400 Unternehmen in über 30 Ländern bei rund 3 Millionen Anwendern im Einsatz. Cryptshare wurde 2017 mit dem „Cybersecurity Excellence Award“ in der Kategorie „E-Mail Security“ ausgezeichnet.
Weitere Informationen finden sich unter www.cryptshare.com. Anwender können sich auch im Blog informieren.

Pressekontakt:
phronesis PR GmbH
Marcus Ehrenwirth, Marcus Wenning
Kobelweg 12 ¼
D-86156 Augsburg
Telefon: +49 821 444800
E-Mail: info@phronesis.de

Web: www.phronesis.de

befine Solutions AG – The Cryptshare Company
Oliver Gäng – Chief Marketing Officer
Schwarzwaldstraße 151
D-79102 Freiburg im Breisgau
Telefon: +49 761 389130
E-Mail: oliver.gaeng@cryptshare.com
Web: www.cryptshare.com